

What is claimed is:

- 1 1. A system for providing a framework for network appliance
2 management in a distributed computing environment, comprising:
3 an appliance status table recording a status report periodically received
4 from each of a plurality of network appliances, each status report containing
5 health and status information and application-specific data for each network
6 appliance; and
7 a catalog server maintaining configuration settings for each network
8 appliance progressively assembled concurrent to providing installable
9 components and dynamically providing a catalog listing currently installable
10 components for each network appliance based on the configuration settings.
- 1 2. A system according to Claim 1, further comprising:
2 a network operations center establishing a secure session with each
3 network appliance.
- 1 3. A system according to Claim 1, further comprising:
2 a network operations center installing an initial set of installable
3 components on each network appliance during a bootstrap configuration.
- 1 4. A system according to Claim 1, wherein the currently installable
2 components comprise at least one self-installable package, further comprising:
3 a component server supplying the at least one package for installation
4 responsive to a request from one such network appliance.
- 1 5. A system according to Claim 4, further comprising:
2 a crypto module digitally signing the at least one package for the network
3 operations center prior to being supplied for installation.
- 1 6. A system according to Claim 4, further comprising:
2 a crypto module encrypting the at least one package prior to being
3 supplied for installation.

1 7. A system according to Claim 1, wherein the installable
2 components comprise at least one file, further comprising:
3 a component server supplying the at least one file responsive to a request
4 from one such network appliance.

1 8. A system according to Claim 7, wherein the component server
2 establishes a secure session prior to the at least one file being supplied for
3 installation.

1 9. A system according to Claim 7, further comprising:
2 a file information subdirectory specifying installation instructions for the
3 at least one file in a pre-determined entry prior to the at least one file being
4 supplied for installation.

1 10. A system according to Claim 1, further comprising:
2 a proxy component server staging the currently installable components for
3 retrieval in a separate components database.

1 11. A system according to Claim 1, wherein the distributed computing
2 environment is TCP/IP-compliant.

1 12. A method for providing a framework for network appliance
2 management in a distributed computing environment, comprising:
3 recording a status report periodically received from each of a plurality of
4 network appliances, each status report containing health and status information
5 and application-specific data for each network appliance;
6 maintaining configuration settings for each network appliance
7 progressively assembled concurrent to providing installable components; and
8 dynamically providing a catalog listing currently installable components
9 for each network appliance based on the configuration settings.

1 13. A method according to Claim 12, further comprising:
2 establishing a secure session with each network appliance.

1 14. A method according to Claim 12, further comprising:
2 installing an initial set of installable components on each network
3 appliance during a bootstrap configuration.

1 15. A method according to Claim 12, wherein the currently installable
2 components comprise at least one self-installable package, further comprising:
3 supplying the at least one package for installation responsive to a request
4 from one such network appliance.

1 16. A method according to Claim 15, further comprising:
2 digitally signing the at least one package prior to being supplied for
3 installation.

1 17. A method according to Claim 15, further comprising:
2 encrypting the at least one package prior to being supplied for installation.

1 18. A method according to Claim 12, wherein the installable
2 components comprise at least one file, further comprising:
3 supplying the at least one file responsive to a request from one such
4 network appliance.

1 19. A method according to Claim 18, further comprising:
2 establishing a secure session prior to the at least one file being supplied for
3 installation.

1 20. A method according to Claim 18, further comprising:
2 specifying installation instructions for the at least one file in a pre-
3 determined entry prior to the at least one file being supplied for installation.

1 21. A method according to Claim 12, further comprising:
2 staging the currently installable components for retrieval in a separate
3 components database.

1 22. A method according to Claim 12, wherein the distributed
2 computing environment is TCP/IP-compliant.

1 23. A computer-readable storage medium holding code for performing
2 the method according to Claims 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, or 22.

1 24. A system for autonomously managing a network appliance
2 deployed within a distributed computing environment, comprising:
3 an internal catalog of components installed on one such network appliance
4 identified by component and version; and
5 a status daemon periodically providing a status report containing health
6 and status information and application-specific data for the one such network
7 appliance; and
8 a catalog checker obtaining a catalog of currently installable components
9 dynamically generated for the one such network appliance and determining non-
10 current components by comparing the components and versions listed in the
11 obtained catalog against the internal catalog.

1 25. A system according to Claim 24, further comprising:
2 a network operations center negotiating a secure connection with the one
3 such network appliance.

1 26. A system according to Claim 24, further comprising:
2 an initial plug-in executed on the one such network appliance.

1 27. A system according to Claim 24, further comprising:
2 a post plug-in executed on the one such network appliance.

1 28. A system according to Claim 24, further comprising:
2 a network operations center broadcasting a query message to each such
3 network appliance to trigger a status report.

1 29. A system according to Claim 24, wherein the components
2 comprise at least one self-installable package, further comprising:

3 an installer obtaining the at least one self-installable package and installing
4 the at least one self-installable package per instructions encoded therein.

1 30. A system according to Claim 29, wherein the components further
2 comprise at least one file dependent on the at least one self-installable package,
3 further comprising:

4 an installer obtaining the at least one file subsequent to installing the at
5 least one self-installable package and installing the at least one self-installable
6 package per instructions stored in a pre-determined entry.

1 31. A system according to Claim 29, further comprising:
2 a component server negotiating a non-secure session prior to obtaining the
3 at least one self-installable package.

1 32. A system according to Claim 29, further comprising:
2 a crypto module at least one of authenticating and decrypting the at least
3 one self-installable package prior to installing the at least one self-installable
4 package.

1 33. A system according to Claim 29, wherein the instructions comprise
2 an executable installation program plus one or more files to be installed.

1 34. A system according to Claim 29, wherein the components further
2 comprise at least one file, further comprising:

3 an installer obtaining the at least one file and installing the at least one
4 self-installable package per instructions stored in a pre-determined entry.

1 35. A system according to Claim 34, further comprising:
2 a component server negotiating a secure session prior to obtaining the at
3 least one self-installable package.

1 36. A system according to Claim 34, wherein the pre-determined entry
2 comprise a file information subdirectory identifying installation instructions.

1 37. A system according to Claim 29, wherein at least one such network
2 appliance performs one of electronic mail anti-virus scanning, content filtering,
3 packet routing, and file, Web and print servicing.

1 38. A system according to Claim 29, wherein the distributed
2 computing environment is TCP/IP-compliant.

1 39. A method for autonomously managing a network appliance
2 deployed within a distributed computing environment, comprising:
3 maintaining an internal catalog of components installed on one such
4 network appliance identified by component and version;
5 periodically providing a status report containing health and status
6 information and application-specific data for the one such network appliance;
7 obtaining a catalog of currently installable components dynamically
8 generated for the one such network appliance; and
9 determining non-current components by comparing the components and
10 versions listed in the obtained catalog against the internal catalog.

1 40. A method according to Claim 39, further comprising:
2 negotiating a secure connection with the one such network appliance.

1 41. A method according to Claim 39, further comprising:
2 executing an initial plug-in on the one such network appliance.

1 42. A method according to Claim 39, further comprising:
2 executing a post plug-in on the one such network appliance.

1 43. A method according to Claim 39, further comprising:
2 broadcasting a query message to each such network appliance to trigger a
3 status report.

1 44. A method according to Claim 39, wherein the components
2 comprise at least one self-installable package, further comprising:
3 obtaining the at least one self-installable package; and

4 installing the at least one self-installable package per instructions encoded
5 therein.

1 45. A method according to Claim 44, wherein the components further
2 comprise at least one file dependent on the at least one self-installable package,
3 further comprising:

4 obtaining the at least one file subsequent to installing the at least one self-
5 installable package; and

6 installing the at least one self-installable package per instructions stored in
7 a pre-determined entry.

1 46. A method according to Claim 44, further comprising:
2 negotiating a non-secure session prior to obtaining the at least one self-
3 installable package.

1 47. A method according to Claim 44, further comprising:
2 at least one of authenticating and decrypting the at least one self-
3 installable package prior to installing the at least one self-installable package.

1 48. A method according to Claim 44, wherein the instructions
2 comprise an executable installation program plus one or more files to be installed.

1 49. A method according to Claim 39, wherein the components further
2 comprise at least one file, further comprising:
3 obtaining the at least one file; and
4 installing the at least one self-installable package per instructions stored in
5 a pre-determined entry.

1 50. A method according to Claim 49, further comprising:
2 negotiating a secure session prior to obtaining the at least one self-
3 installable package.

1 51. A method according to Claim 49, wherein the pre-determined entry
2 comprise a file information subdirectory identifying installation instructions.

1 52. A method according to Claim 39, wherein at least one such
2 network appliance performs one of electronic mail anti-virus scanning, content
3 filtering, packet routing, and file, Web and print servicing.

1 53. A method according to Claim 39, wherein the distributed
2 computing environment is TCP/IP-compliant.

1 54. A computer-readable storage medium holding code for performing
2 the method according to Claims 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51,
3 52, or 53.

205210 20295007